

## REMARKS

Applicants appreciate the detailed examination evidenced by the Official Action mailed March 2, 2006 (hereinafter "Office Action"). In response, Applicants have amended Claims 28, 31, and 32 to clarify that the common nonce recited therein is "associated with each of the plurality of servers", as recited by Claim 1. In addition, Claims 2 and 30 have been amended to clarify that the common nonce is generated "by an entity other than the client or the plurality of servers". Support for these amendments are provided in the specification as originally filed, for example, at Page 8, lines 24-26, and Figures 1A-B. As such, no new matter has been added.

Accordingly, Applicants respectfully submit that pending Claims 1-32 are patentable over the cited references for at least the reasons discussed below.

### **Independent Claims 1, 26-28, 31 and 32 Are Patentable Over Brezak and Ganesan**

Independent Claims 1, 26-28, 31 and 32 stand rejected under 35 U.S.C. §103(a) as obvious over U.S. Patent Application Publication No. 2003/0018913 to Brezak et al. (hereinafter "Brezak") in view of U.S. Patent 5,535,276 to Ganesan (hereinafter "Ganesan"). Claim 1, for example, recites:

A method for a middle-tier server to impersonate a client to a plurality of servers, the method comprising:  
    obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers;  
    providing the common nonce to the client;  
    receiving the common nonce signed by the client at the middle-tier server; and  
    providing the signed common nonce to the plurality of servers as a signature for transactions so as to authenticate the client to the plurality of servers. (*Emphasis added*).

The Office Action asserts that Brezak discloses all of the recitations of Claim 1 with the exception of "the client signing the common nonce (PAC)", which the Office Action asserts is disclosed by Ganesan. *See* Office Action, Page 3. As such, the Office Action appears to assert that the privilege attribute certificate (PAC) of Brezak is equivalent to "a common nonce associated with each of the plurality of servers", as recited by Claim 1. For example, the Office Action asserts that Brezak discloses obtaining a common nonce associated with each of the plurality of servers in Paragraphs 0043 and 0049. *See* Office Action, Page 3.

Brezak appears to disclose a system for controlling delegation of authentication credentials so that a server A 210 may access a plurality of servers B 212, C 214, and D 216 on behalf of a client 202. *See* Brezak, Abstract and Fig. 2. In describing the PAC, Brezak provides:

In certain implementations, for example, TGS\_REP message 232 identifies the targeted server/service and client 202, and further includes implementation-specific identity/user/client account data, e.g., in the form of a privilege attribute certificate (PAC), a security identifier, a Unix ID, Passport ID, a certificate, etc. A PAC, for example, may be generated by authentication service 206, or simply copied from the client's service ticket that was included in TGS\_REQ message 230.

Brezak, Paragraph 0049 (*emphasis added*). In other words, the reply message 232 (TGS\_REP) from the authentication server 206 includes a PAC, which may be generated by the authentication server 206 and/or copied from the client's service ticket included in the request message 230 (TGS\_REQ). The PAC may include identity/user/client account data, and as such, is presumably associated with the client 202.

In addition, in Paragraph 0043, Brezak provides:

When client 202 wants to access server A 210, the client sends a ticket granting service request (TGS\_REQ) message 224 to authentication service 206, which returns a ticket granting service reply (TGS\_REP) message 226. TGS\_REP message 226 includes a service ticket associated with client 202 and server A 210. Subsequently, to initiate a communication session, client 202 forwards the service ticket to server A 210, in an application protocol request (AP\_REQ) message 228. Such processes/procedures are well known, and as such are not disclosed herein in greater detail.

Brezak, Paragraph 0043 (*emphasis added*). In other words, TGS\_REP message 226 from the authentication server 206 includes a service ticket that is associated with the client 202 and one of the servers, *i.e.*, server A 210.

In contrast, Claim 1 recites "a common nonce associated with *each* of the *plurality of servers*". Applicants submit that neither the PAC nor the service ticket described in the cited portions of Brezak appears to be associated with *each* of the plurality of servers A 210, B 212, C 214, and D 216 of Figure 2. *See* Brezak, Fig. 2. Rather, as noted above, the PAC

(included in TGS\_REQ message **230** and/or TGS\_REP message **232**) includes client account data, and as such, appears to be associated with the client **202**. Likewise, the service ticket included in the message **226** is associated with server A **210**. Thus, nowhere do the cited portions of Brezak disclose or suggest that the PAC included in message **232** or the service ticket included in message **226** is associated with each of the plurality of servers A **210**, B **212**, C **214**, and D **216**.

Accordingly, Applicants submit that Brezak does not appear to disclose or suggest "a common nonce associated with each of the plurality of servers", as recited by Claim 1. If the Examiner continues to maintain the present rejections based on Brezak, Applicants respectfully request that the Examiner point to specific portions of Brezak that disclose or suggest a common nonce that is "associated with each of the plurality of servers", as recited by Claim 1.

Moreover, the Office Action does not appear to rely on Ganesan to disclose or suggest such a common nonce associated with each of a plurality of servers. *See* Office Action, Page 3. Rather, Ganesan appears to be directed to split private key asymmetric cryptography, and is relied upon to show that a message, including a ticket to access a server **50**, is encrypted/signed and then verified to authenticate a client **10** to the server **50**. *See* Ganesan, Col. 5, lines 34-56 and Col. 15, lines 45-60.

Accordingly, as the cited portions of Brezak and Ganesan do not appear to disclose or suggest "a common nonce associated with each of the plurality of servers", Applicants submit that Claim 1 is patentable over the combination of Brezak and Ganesan. Claims 26-28, 31, and 32 as amended similarly recite such a common nonce, and are thus patentable for similar reasons. Also, dependent claims 2-25 and 29-30 are patentable at least per the patentability of Claims 1 and 28 from which they respectively depend.

#### **Many of the Dependent Claims Are Separately Patentable**

Applicants submit that dependent Claims 2-25 and 29-30 are patentable at least by virtue of the patentability of independent Claims 1 and 28 from which they respectively depend. Applicants further submit that several of the dependent claims are also separately

patentable. For example, Claim 2 as amended recites, in part, that obtaining a common nonce comprises "generating, by an entity other than the client or the plurality of servers, a common nonce based on information obtained from each of the plurality of servers". The Office Action asserts that the recitations of Claim 2 are disclosed by Ganesan at Col. 5, lines 34-56. See Office Action, Page 6. However, as provided by the cited portion of Ganesan:

Having verified the authenticity of the tgs\_req, the server 40 responds with Message 4,

$$\text{tgs\_rep: } \{Kc,s, \text{time\_exp}, n, s, \dots\} Kc, \text{tgs}\{Tc,s\}Ks$$

This message is very similar in structure and purpose to the as\_rep message. The first part consists of a session key, expiry time, etc., encrypted with Kc,tgs. The client computer 10 can decrypt this to recover the session key and other information. The second portion is a ticket to access the server 50, encrypted with the long term key Ks shared by the server 50 and the server 40. The client using computer 10 now constructs Message 5 and sends it to the server 50, as follows:

$$\text{ap\_rep: } \{ts, ck, \dots\} Kc, s\{Tc, s\} Ks$$

This message is similar to the tgs\_req, in that it contains an encrypted ticket  $\{Tc,s\}Ks$  which the server 50 can use to recover Tc,s, which authenticates the client to the server 50 and, among other information, contains the session key Kc,s. The server 50 then uses Kc,s to decrypt the first part of the message, the authenticator, which has a time-stamp, ts, a check-sum, ck, etc.

Ganesan Col. 5, lines 34-56 (*emphasis added*). In other words, Ganesan describes that a server 40 generates Message 4, which includes a ticket (encrypted with a shared long-term key Ks) to access server 50. After receiving Message 4, a client 10 generates Message 5, which includes the encrypted ticket to authenticate the client 10 to the server 50. As such, Ganesan describes authentication between a client 10 and a *single* server 50 via a secure environment, which includes a server 40.

Ganesan provides a more general description of the above operations at Col. 4:

The fundamental message exchanges are shown in FIG. 1. In message 1 the user uses a personal computer or workstation 10 to request a ticket granting ticket (TGT) from an authentication server (AS) 20. The server 20 creates such a ticket TGT, looks up the user's password from the

Kerberos database 30, encrypts the TGT with the password and sends it to the user via the computer 10 in message 2. The user decrypts the TGT with her password using computer 10, and stores the TGT on computer 10, for example on a hard disk or in the random access memory (RAM). Then, when the user desires to access a service, she sends message 3, which contains the TGT to the ticket granting server 40. The server 40 verifies the TGT and sends back, in message 4, a service ticket to access the service server 50, and a session key, encrypted with the user's password retrieved from database 30. In message 5 the user presents via computer 10 the service ticket to the server 50, which verifies it and also recovers the session key from it. If mutual authentication is required, the server 50, in message 6, sends back a message encrypted with the session key. All communications between servers 20, 40 and 50 and computer 10 are via network 60. All communications between servers 20 and 40 and database 30 are preferably by direct communications link.

Ganesan, Col. 4, lines 11-34 (*emphasis added*). Accordingly, Ganesan describes a first ticket TGT, which is generated by an authentication server 20, and a second ticket (used to access server 50), which is generated by the ticket granting server 40. The Office Action appears to assert that one or more of the tickets of Ganesan is equivalent to "a common nonce" that is generated "based on information obtained from each of the plurality of servers", as recited by Claim 2 as amended. *See Office Action, Page 6.*

As an initial matter, Applicants submit that, as shown in Figure 1, Ganesan illustrates authentication between a client 10 and a *single* server 50, and as such, does not appear to disclose or suggest generating a ticket based on information obtained from a *plurality* of servers. *See Ganesan, Fig. 1.* Moreover, even if one were to consider the secure servers 20 and/or 40 along with the server 50 as the plurality of servers to which the client 10 is authenticated, the tickets described in Ganesan do not appear to be generated based on information obtained from *each* of the plurality of servers 20, 40, and 50. Rather, as noted above, the ticket TGT appears to be generated by server 20 independent of information from the servers 40 and 50. Likewise, the ticket to access server 50 appears to be generated by server 40 independent of information from server 20. Thus, Ganesan does not disclose or suggest generating a ticket based on information from *each* of the servers 20, 40, and 50. In addition, as the tickets are generated by servers 20 and/or 40, Ganesan also does not disclose or suggest generating the common nonce by an entity *other than* the client or the plurality of

In re: McGarvey et al.  
Serial No.: 09/921,536  
Filed: August 3, 2001  
Page 14

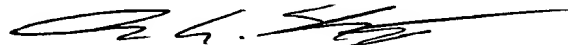
servers.

Thus, the cited portions of Ganesan do not disclose or suggest "generating, by an entity other than the client or the plurality of servers, a common nonce based on information obtained from each of the plurality of servers", as recited by Claim 2 as amended. Nor does the Office Action appear to rely on the other cited references as disclosing these recitations. Accordingly, Applicants submit that Claim 2 is separately patentable over the cited references for at least these reasons. Claim 30 contains similar recitations, and as such, is separately patentable for at least similar reasons.

### **Conclusion**

Accordingly, based on the amendments and remarks provided above, Applicants submit that pending Claims 1-32 are in condition for allowance, which is respectfully requested. Applicants encourage the Examiner to contact the undersigned by telephone to resolve any remaining issues.

Respectfully submitted,



Rohan G. Sabapathypillai  
Registration No. 51,074

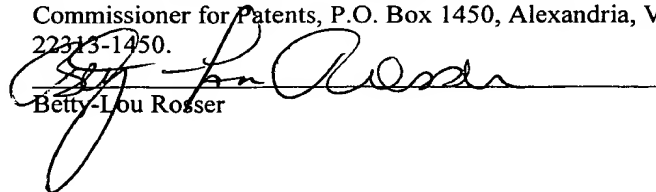
USPTO Customer No. 20792  
Myers Bigel Sibley & Sajovec, P.A.  
Post Office Box 37428  
Raleigh, NC 27627  
Telephone (919) 854-1400  
Facsimile (919) 854-1401

### **CERTIFICATE OF EXPRESS MAILING**

Express Mail Label No. EV854924371US

Date of Deposit: June 2, 2006

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to MAIL STOP Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA, 22313-1450.



Betty-Lou Rosser